

CORPORATE ACCOUNT TERMINATION AND DELETION PROCEDURE

1. PURPOSE

This procedure has been established to define the steps to be followed for the deletion of corporate digital accounts (e-mail, authentication, system access credentials, etc.) and the secure destruction of data at the end of the service period or when authorization is revoked.

2. SCOPE

This procedure covers all user accounts assigned by Alanya Alaaddin Keykubat University that provide access to the following systems:

Corporate e-mail services

- (e.g., name.surname@alanya.edu.tr / studentnumber@ogr.alanya.edu.tr)
 - Active Directory/LDAP and SSO authentication systems
 - VPN and all network resources
 - University software (Student Information System, e-signature, etc.)
 - Cloud services (Google Workspace, Microsoft 365, etc.)
-

3. LEGAL AND STANDARD REFERENCES

- ISO/IEC 27001:2013
 - Law No. 6698 on the Protection of Personal Data (KVKK)
 - Official Gazette No. 30922: Regulation on State Archive Services
-

4. DEFINITIONS

- **Deletion:** Permanent removal of user data associated with the account from the systems.
 - **Asset Owner:** The unit manager or data controller associated with the account.
 - **Authorized Access:** Access that may be performed by authorized users before the deletion process is completed.
-

5. PROCESS STEPS

5.1 Reasons for Account Termination

- Resignation, retirement, transfer to another institution, or disassociation of personnel
- Graduation, withdrawal, or departure of a student from the university
- Termination of the service contract
- Due to security reasons (incident detection, misuse, etc.)

5.2 Account Deletion

- The account is permanently deleted 6 months after the information about the departure of the personnel or student is received.
- Deletion process:
 - Includes e-mail and cloud data (Google Drive, OneDrive, etc.);
 - All data within Google applications (Drive, Gmail, Calendar, Meet, Chat, Keep, Sites, Forms, Groups, Photos, Tasks, Jamboard, Contacts) and associated Google licenses
 - Cancellation of Microsoft licenses (such as Microsoft 365 licenses), termination of access to applications like Outlook, Word, Excel, PowerPoint, Teams, OneDrive, SharePoint, OneNote, Planner, To Do, and Forms, and deletion of all data within these applications.

5.3 Revocation of Access Rights

- All system, application, and network access rights are revoked.
- The user is removed from user groups and disconnected from the authentication system.
- Mobile device pairings, individual sessions, and VPN certificates are canceled.

5.4 Account Retention Period

Account Type	Retention Period	Service Type	Notes
Student Accounts	6 Months	Corporate e-mail services, Cloud services, Active Directory/LDAP and SSO authentication systems, VPN and network resources, University software	Notification is provided for graduate accounts.
Staff Accounts	6 Months	Corporate e-mail services, Cloud services, Active Directory/LDAP and SSO authentication systems, VPN and network resources, University software	Notification is provided for staff accounts.

6. DATA MANAGEMENT AND BACKUP

6.1 Backup Responsibility

- The university and the Information Technology Department are not responsible for backing up user data.
 - Users must export their personal data and academic content before the end of their term.
 - At the end of the allocated period (6 months), all data on the system will be permanently deleted.
-

7. NOTIFICATION AND RECORDING

- Prior to the deletion process, the user is notified via corporate e-mail and personal e-mail or SMS.
 - After deletion, the process is recorded in the ISMS inventory and the registration system.
-